KOMMISSIONENS BESLUT

av den 4 maj 2010

om en säkerhetsplan för driften av informationssystemet för viseringar

(2010/260/EU)

EUROPEISKA KOMMISSIONEN HAR ANTAGIT DETTA BESLUT

med beaktande av fördraget om Europeiska unionens funktionssätt,

med beaktande av Europaparlamentets och rådets förordning (EG) nr 767/2008 av den 9 juli 2008 om informationssystemet för viseringar (VIS) och utbytet mellan medlemsstaterna av uppgifter om viseringar för kortare vistelse (VIS-förordningen) [1], särskilt artikel 32, och

av följande skäl:

(1) I artikel 32.3 i förordning (EG) nr 767/2008 föreskrivs att förvaltningsmyndigheten, med avseende på driften av VIS, ska vidta de åtgärder som är nödvändiga för att uppnå de mål som anges i punkt 2, inbegripet anta en dataskyddsplan.

(2) I artikel 26.4 i förordning (EG) nr 767/2008 föreskrivs att kommissionen ska ha ansvar för den operativa förvaltningen av VIS under en övergångsperiod innan förvaltningsmyndigheten övertar ansvaret.

(3) Europaparlamentets och rådets förordning (EG) nr 45/2001 [2] är tillämplig på kommissionens behandling av personuppgifter när den utövar sitt ansvar i samband med den operativa förvaltningen av VIS.

(4) I artikel 26.7 i förordning (EG) nr 767/2008 föreskrivs att om kommissionen delegerar sitt ansvar under övergångsperioden innan förvaltningsmyndigheten övertar ansvaret, ska den säkerställa att delegeringen inte inverkar negativt på någon av de kontrollmekanismer som följer av unionsrätten, oavsett om de utgörs av domstolen, revisionsrätten eller Europeiska datatillsynsmannen.

(5) Förvaltningsmyndigheten bör utarbeta en egen säkerhetsplan för VIS när den har börjat utöva sitt ansvar.

(6) De skyddstjänster som krävs för VIS-nätet har beskrivits i kommissionens beslut 2008/602/EG av den 17 juni 2008 om fastställande av fysisk arkitektur och krav för de nationella gränssnitten och för kommunikationsinfrastrukturen mellan det centrala VIS och de nationella gränssnitten under utvecklingsfasen [3].

(7) I artikel 27 i förordning (EG) nr 767/2008 anges att den ordinarie delen av det centrala VIS, som står för teknisk tillsyn och administration, ska vara belägen i Strasbourg (Frankrike) och en reserv för det centrala VIS, varigenom alla funktioner i den ordinarie delen av det centrala VIS säkerställs om detta system skulle sluta fungera, ska ligga i Sankt Johann im Pongau (Österrike).

(8) De säkerhetsansvarigas uppgifter bör fastslås för att säkerställa snabba och effektiva åtgärder samt rapportering vid säkerhetstillbud.

(9) Det bör utarbetas en säkerhetsplan som tar upp alla tekniska och organisatoriska detaljer i enlighet med bestämmelserna i detta beslut.

(10) Det bör fastställas åtgärder för att säkerställa en lämplig säkerhetsnivå med avseende på driften av VIS.

HÄRIGENOM FÖRESKRIVS FÖLJANDE.

KAPITEL I

ALLMÄNNA BESTÄMMELSER

Artikel 1

Tillämpningsområde

Genom detta beslut införs den skyddsorganisation och de åtgärder (dataskyddsplan) som avses i artikel 32.3 i förordning (EG) nr 767/2008.

KAPITEL II

ORGANISATION, ANSVARSOMRÅDEN OCH TILLBUDSHANTERING

Artikel 2

Kommissionens uppgifter

1. Kommissionen ska säkerställa och övervaka att de säkerhetsåtgärder avseende det centrala VIS och kommunikationsinfrastrukturen som anges i detta beslut fungerar effektivt.

[1] EUT L 218, 13.8.2008, s. 60.
[2] EGT L 8, 12.1.2001, s. 1.
[3] EUT L 194, 23.7.2008, s. 3.

2. Kommissionen ska utse en säkerhetsansvarig för systemet bland sina tjänstemän. Systemets säkerhetsansvarige ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet. Uppgifterna för systemets säkerhetsansvarige ska särskilt omfatta

a) förberedelse, uppdatering och översyn av den säkerhetsplan som beskrivs i artikel 7 i detta beslut,

b) övervakning av att säkerhetsprocedurerna för det centrala VIS och kommunikationsinfrastrukturen genomförs effektivt,

c) bidra till utarbetandet av rapporter om säkerheten i enlighet med artikel 50.3 och 50.4 i förordning (EG) nr 767/2008,

d) ansvara för samordning och stöd i samband med den kontroll och revision som europeiska datatillsynsmannen utför i enlighet med artikel 42 i förordning (EG) nr 767/2008,

e) övervaka att detta beslut och säkerhetsplanen tillämpas korrekt och fullständigt av eventuella uppdragstagare och underleverantörer som på något sätt deltar i förvaltningen och driften av VIS,

f) föra en förteckning över enskilda nationella kontaktpunkter för säkerhetsfrågor rörande VIS och ställa den till förfogande för de lokalt säkerhetsansvariga för det centrala VIS och för kommunikationsinfrastrukturen.

Artikel 3

Den lokalt säkerhetsansvarige för det centrala VIS

1. Utan att det påverkar tillämpningen av artikel 8 ska kommissionen bland sina tjänstemän utse en lokalt säkerhetsansvarig för det centrala VIS. Intressekonflikter mellan den lokalt säkerhetsansvariges åtaganden och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige för det centrala VIS ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet.

2. Den lokalt säkerhetsansvarige för det centrala VIS ska se till att de säkerhetsåtgärder som det hänvisas till i detta beslut genomförs och att de säkerhetsprocedurer som gäller för den ordinarie delen av det centrala VIS följs. När det gäller reservsystemet för det centrala VIS ska den lokalt säkerhetsansvarige se till att de säkerhetsåtgärder som det hänvisas till i detta beslut, med undantag för dem som anges i artikel 10, genomförs och att de säkerhetsprocedurer som gäller för reservsystemet genomförs.

3. Den lokalt säkerhetsansvarige för det centrala VIS får delegera sina arbetsuppgifter till underställd personal. Intressekonflikter mellan skyldigheten att utföra dessa uppgifter och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige eller dennes tjänstgörande underordnade ska när som helst kunna nås via ett särskilt telefonnummer och en särskild adress.

4. Den lokalt säkerhetsansvarige för det centrala VIS ska utföra de uppgifter som är knutna till sådana säkerhetsåtgärder som ska vidtas på platserna för den ordinarie delen av det centrala VIS respektive för reservsystemet, inom de ramar som fastställs i punkt 1, vilket särskilt innebär att han eller hon ska

a) utföra säkerhetsuppgifter i samband med driften lokalt, inklusive kontroll av brandväggar, regelbundna säkerhetstester, översyn och rapportering,

b) övervaka kontinuitetsplanens effektivitet och se till att regelbundna övningar genomförs,

c) säkra bevis för och rapportera till systemets säkerhetsansvarige om alla tillbud som kan påverka säkerheten för det centrala VIS eller kommunikationsinfrastrukturen,

d) underrätta systemets säkerhetsansvarige om säkerhetsplanen behöver ändras,

e) övervaka att detta beslut och skyddsstrategin tillämpas av eventuella uppdragstagare och underleverantörer som på något sätt är involverade i förvaltningen och driften av det centrala VIS,

f) se till att personalen informeras om sina skyldigheter och övervaka tillämpningen av skyddsstrategin,

g) övervaka utvecklingen när det gäller it-säkerhet och se till att personalen får nödvändig fortbildning,

h) förbereda underlag och alternativ när det gäller att införa, uppdatera och se över skyddsstrategin i enlighet med artikel 7.

Artikel 4

Lokalt säkerhetsansvarig för kommunikationsinfrastrukturen

1. Utan att det påverkar tillämpningen av artikel 8 ska kommissionen bland sina tjänstemän utse en lokalt säkerhetsansvarig för kommunikationsinfrastrukturen. Intressekonflikter mellan den lokalt säkerhetsansvariges åtaganden och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska utses av generaldirektören för kommissionens generaldirektorat för rättvisa, frihet och säkerhet.

2. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska övervaka kommunikationsinfrastrukturens funktion och se till att säkerhetsåtgärderna genomförs och säkerhetsförfarandena följs.

3. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen får delegera sina arbetsuppgifter till underställd personal. Intressekonflikter mellan skyldigheten att utföra dessa uppgifter och varje annat officiellt åtagande ska undvikas. Den lokalt säkerhetsansvarige eller dennes tjänstgörande underordnade ska när som helst kunna nås via ett särskilt telefonnummer och en särskild adress.

4. Den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen ska utföra sådana uppgifter som är förbundna med säkerhetsåtgärder rörande kommunikationsinfrastrukturen, särskilt

a) alla säkerhetsuppgifter som rör kommunikationsinfrastrukturen, inklusive kontroll av brandväggar, regelbundna säkerhetstester, översyn och rapportering,

b) övervaka kontinuitetsplanens effektivitet och se till att regelbundna övningar genomförs,

c) säkra bevis för och rapportera till systemets säkerhetsansvarige om alla tillbud som kan påverka säkerheten i det centrala VIS, kommunikationsinfrastrukturen eller de nationella systemen,

d) underrätta systemets säkerhetsansvarige om säkerhetsplanen behöver ändras,

e) övervaka att detta beslut och skyddsstrategin tillämpas av eventuella uppdragstagare och underleverantörer som på något sätt deltar i förvaltningen av kommunikationsinfrastrukturen,

f) se till att personalen informeras om sina skyldigheter och övervaka tillämpningen av säkerhetsplanen,

g) övervaka utvecklingen när det gäller it-säkerhet och se till att personalen får nödvändig fortbildning,

h) förbereda underlag och alternativ när det gäller att införa, uppdatera och se över skyddsstrategin i enlighet med artikel 7.

Artikel 5

Säkerhetstillbud

1. Varje händelse som har eller kan få en inverkan på säkerheten i samband med driften av VIS och riskerar att orsaka skada eller förluster för VIS ska anses som ett säkerhetstillbud, särskilt om systemet har utsatts för dataintrång eller om uppgifternas tillgänglighet, integritet och konfidentialitet har äventyrats eller kan ha äventyrats.

2. Säkerhetsplanen ska fastställa förfaranden för att få situationen att återgå till det normala efter ett tillbud. Säkerhetstillbud ska hanteras på ett sätt som säkerställer snabba, effektiva och välavvägda insatser.

3. Information om ett säkerhetstillbud som har eller kan ha en inverkan på driften av VIS i en medlemsstat, eller på tillgången till eller integriteten eller konfidentialiteten hos VIS-uppgifter som matats in av en medlemsstat, ska vidarebefordras till den berörda medlemsstaten. Säkerhetstillbud ska rapporteras till kommissionens uppgiftsskyddsombud.

Artikel 6

Hantering av tillbud

1. All personal och alla uppdragstagare som arbetar med att utveckla, förvalta eller driva VIS ska vara skyldiga att notera och rapportera eventuella iakttagna eller misstänkta säkerhetsbrister i driften av VIS till systemets säkerhetsansvarige, den lokalt säkerhetsansvarige för det centrala VIS eller den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen, beroende på omständigheterna.

2. Vid ett tillbud som har eller kan ha en inverkan på säkerheten i samband med driften av VIS ska den lokalt säkerhetsansvarige för det centrala VIS eller den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen snarast möjligt underrätta systemets säkerhetsansvarige och, i tillämpliga fall, den nationella kontaktpunkten för säkerhetsfrågor rörande VIS, om det finns en sådan kontaktpunkt i medlemsstaten i fråga; detta meddelande ska vara skriftligt, men om särskild skyndsamhet är påkallad får även andra kommunikationsmedel användas. Rapporten ska innehålla en beskrivning av säkerhetstillbudet, risknivån, de möjliga konsekvenserna och de åtgärder som har vidtagits eller bör vidtas för att minska risken.

3. Eventuella bevis med anknytning till säkerhetstillbudet ska säkras omedelbart av antingen den lokalt säkerhetsansvarige för det centrala VIS eller den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen, beroende på omständigheterna. I den utsträckning det är möjligt enligt de tillämpliga bestämmelserna om uppgiftsskydd ska sådan bevisning göras tillgänglig för systemets säkerhetsansvarige på dennes begäran.

4. Återkopplingsprocesser ska användas för att säkerställa att information om resultaten förs vidare efter det att tillbudet har hanterats och säkerhetsinsatserna avslutats.

KAPITEL III

SÄKERHETSÅTGÄRDER

Artikel 7

Säkerhetsplan

1. Generaldirektören för generaldirektoratet för rättvisa, frihet och säkerhet ska fastställa, uppdatera och regelbundet se över en bindande säkerhetsplan i enlighet med detta beslut. Säkerhetsplanen ska omfatta detaljerade förfaranden och åtgärder för att skydda VIS tillgänglighet, integritet och konfidentialitet, inklusive krisberedskap, i syfte att säkerställa en lämplig säkerhetsnivå i enlighet med detta beslut. Säkerhetsplanen ska vara utformad på ett sätt som överensstämmer med detta beslut.

2. Säkerhetsplanen ska grunda sig på en riskanalys. De åtgärder som beskrivs i säkerhetsplanen ska stå i proportion till de identifierade riskerna.

3. Riskanalysen och säkerhetsplanen ska uppdateras om det blir nödvändigt på grund av tekniska förändringar, nya hot eller andra omständigheter. Säkerhetsplanen ska under alla omständigheter ses över årligen för att säkerställa att den fortfarande överensstämmer med den senaste riskanalysen eller eventuella andra nyligen konstaterade tekniska förändringar, hot eller andra relevanta omständigheter.

4. Säkerhetsplanen ska utarbetas av systemets säkerhetsansvarige, i samarbete med den lokalt säkerhetsansvarige för VIS och den lokalt säkerhetsansvarige för kommunikationsinfrastrukturen.

Artikel 8

Genomförandet av säkerhetsåtgärderna

1. Genomförandet av de uppgifter och krav som fastställs i detta beslut och i säkerhetsplanen, inklusive uppgiften att utse en lokalt säkerhetsansvarig, kan läggas ut på eller anförtros privata eller offentliga organisationer.

2. I så fall ska kommissionen genom rättsligt bindande avtal se till att de krav som fastställs i detta beslut och i säkerhetsplanen uppfylls fullt ut. Vid delegering eller utläggning av uppgiften att utse en lokal säkerhetsansvarig ska kommissionen genom rättsligt bindande avtal se till att den ges tillfälle att yttra sig om den person som valet faller på.

Artikel 9

Kontroll av tillträdet till anläggningen

1. Yttre säkerhetsgränser med lämpliga barriärer och inträdeskontroller ska användas för att skydda områden där det finns databehandlingsutrustning.

2. Inom dessa yttre säkerhetsgränser ska det finnas säkerhetszoner för att skydda de fysiska beståndsdelarna (anläggningstillgångar), inklusive hårdvara, databärare och konsoler, men även planer och annan dokumentation över VIS samt kontor och andra arbetsutrymmen för personal som deltar i driften av VIS. Dessa säkerhetszoner ska skyddas genom för ändamålet avpassade tillträdeskontroller för att säkerställa att endast auktoriserad personal ges tillträde. Arbete som utförs inom säkerhetszoner ska omfattas av säkerhetsbestämmelser som fastställs närmare i säkerhetsplanen.

3. Åtgärder ska planeras och vidtas för att säkerställa den fysiska säkerheten med avseende på kontor och andra lokaler och installationer. Lastnings- och avlastningsplatser och andra ställen där obehöriga kan ta sig in på området ska övervakas och, om möjligt, hållas avskilda från databehandlingsinstallationer för att undvika att obehöriga får tillträde.

4. Ett fysiskt skydd för de yttre säkerhetsgränserna mot skador från naturkatastrofer eller katastrofer orsakade av människan ska utformas och användas på ett sätt som står i proportion till den risk som föreligger.

5. Utrustning ska skyddas från fysiska och miljörelaterade hot samt mot risken för obehörigt tillträde.

6. Om kommissionen har tillgång till sådan information ska den komplettera den förteckning som avses i artikel 2.2 f med uppgifter om en kontaktpunkt för övervakning av hur bestämmelserna i denna artikel tillämpas på den plats där reservsystemet för det centrala VIS är placerat.

Artikel 10

Kontroll av databärare och tillgångar

1. Flyttbara databärare som innehåller data ska skyddas mot obehörig åtkomst, missbruk eller förvanskning och vara läsbara under uppgifternas hela livstid.

2. Databärarna ska skaffas undan på ett säkert sätt när de har spelat ut sin roll, i enlighet med de förfaranden som fastställs närmare i säkerhetsplanen.

3. Förteckningar ska säkerställa att uppgifter om lagringsplats, lagringsperioder och åtkomsträttigheter finns tillgängliga.

4. Alla viktiga tillgångar som hör till det centrala VIS och kommunikationsinfrastrukturen ska identifieras, så att de kan skyddas i förhållande till deras betydelse. Ett uppdaterat register över relevant it-utrustning ska föras.

5. Det ska finnas uppdaterad dokumentation rörande det centrala VIS och kommunikationsinfrastrukturen. Denna dokumentation ska skyddas mot obehörig åtkomst.

Artikel 11

Lagringskontroll

1. Lämpliga åtgärder ska vidtas för att säkerställa en säker lagring av uppgifter och förebygga obehörig åtkomst.

2. All utrustning som innehåller lagringsmedier ska antingen kontrolleras för att säkerställa att känsliga uppgifter har avlägsnats eller skrivits över före bortskaffandet, eller förstöras på ett säkert sätt.

Artikel 12

Kontroll av lösenord

1. Alla lösenord ska förvaras säkert och behandlas konfidentiellt. Vid misstanke om att ett lösenord har röjts ska lösenordet omedelbart bytas ut eller användarkontot avaktiveras. Unika och individuella användaridentiteter ska användas.

2. Procedurer för inloggning och utloggning ska fastställas i säkerhetsplanen, i syfte att förhindra obehörig åtkomst.

Artikel 13

Tillträdeskontroll

1. Säkerhetsplanen ska fastställa ett formellt förfarande för registrering och avregistrering av personal, som gör det möjligt att bevilja och återkalla tillträde till VIS-hårdvara och VIS-programvara i det centrala VIS för operativa förvaltningsändamål. Tilldelningen och användningen av nödvändiga åtkomstuppgifter (lösenord eller liknande) ska kontrolleras genom ett formellt förvaltningsförfarande i enlighet med säkerhetsplanen.

2. Tillträdet till VIS-hårdvara och VIS-programvara i det centrala VIS ska

i) vara begränsat till auktoriserade personer,

ii) vara begränsat till fall där det är möjligt att fastställa ett legitimt syfte i enlighet med artiklarna 42 och 50.2 i förordning (EG) nr 767/2008,

iii) inte i tid och omfattning överstiga vad som är nödvändigt för ändamålet för tillträdet, och

iv) endast ske i enlighet med en policy för tillträdeskontroll som ska fastställas i säkerhetsplanen.

3. Endast konsoler och programvara som godkänts av den lokalt säkerhetsansvarige för det centrala VIS får användas vid det centrala VIS. Användningen av hjälpprogram varmed kontrollen av system och applikationer skulle kunna kringgås ska begränsas och kontrolleras. Förfaranden för att kontrollera installationen av programvara ska inrättas.

Artikel 14

Kommunikationskontroll

Kommunikationsinfrastrukturen ska stå under kontroll för att säkerställa tillgänglighet, integritet och konfidentialitet i informationsutbytet. Kryptering ska användas för att skydda de uppgifter som överförs i kommunikationsinfrastrukturen.

Artikel 15

Kontroll av registrering

Konton för personer som givits tillgång till VIS-programvara från det centrala VIS ska övervakas av den lokalt säkerhetsansvarige för det centrala VIS. Användningen av dessa konton, inklusive tidsuppgifter och användaridentitet, ska registreras.

Artikel 16

Kontroll av transport

1. I säkerhetsplanen ska lämpliga åtgärder fastställas för att förhindra obehörig läsning, kopiering, ändring eller radering av personuppgifter vid överföring till eller från VIS eller i samband med transport av databärare. Säkerhetsplanen ska även omfatta bestämmelser om tillåtna former av försändelse eller transport och om ansvarsförfaranden i samband med transport av föremål och deras ankomst till bestämmelseorten. Databärarna ska inte innehålla några andra data än de som ska översändas.

2. Tjänster som tillhandahålls av tredje man, och som rör tillgång till eller behandling, kommunikation eller förvaltning av databehandlingsutrustning, eller syftar till att leverera produkter eller tjänster för databehandlingsutrustning, ska omfattas av lämpliga integrerade säkerhetskontroller.

Artikel 17

Kommunikationsinfrastrukturens säkerhet

1. Kommunikationsinfrastrukturen ska förvaltas och kontrolleras på ett tillfredsställande sätt för att skydda den mot hot och garantera säkerheten för kommunikationsinfrastrukturen i sig och för det centrala VIS, inklusive de uppgifter som utbyts genom den.

2. För alla nätverkstjänster gäller att krav på säkerhetsanordningar, servicenivåer och förvaltning ska fastställas i nätserviceavtalet med tjänsteleverantören.

3. Skyddskraven omfattar inte endast VIS accesspunkter, utan även eventuella andra tjänster som används av kommunikationsinfrastrukturen. Lämpliga åtgärder ska fastställas i säkerhetsplanen.

Artikel 18

Övervakning

1. Information om all konsultation och behandling av uppgifter i det centrala VIS, i den mening som avses i artikel 34.1 i förordning (EG) nr 767/2008, ska registreras och lagras på ett säkert sätt på de platser där det ordinarie systemet respektive reservsystemet för det centrala VIS finns och göras tillgängliga från dessa platser under den period som anges i artikel 34.2 i förordning (EG) nr 767/2008.

2. Förfaranden för att övervaka användningen av och eventuella brister i databehandlingsutrustningen ska fastställas i säkerhetsplanen, och resultaten av övervakningen ska gås igenom regelbundet. Om nödvändigt ska lämpliga åtgärder vidtas.

3. Loggfunktioner och loggar ska skyddas mot manipulation och obehörigt tillträde för att uppfylla kraven på insamling och bevarande av bevismaterial under den för ändamålet föreskrivna perioden.

Artikel 19

Kryptering

Krypteringsmetoder ska användas när det är lämpligt för att skydda information. Användningen av sådana krypteringsmetoder ska, tillsammans med syften och villkor, godkännas på förhand av systemets säkerhetsansvarige.

KAPITEL IV

PERSONALSÄKERHET

Artikel 20

Personalprofiler

1. Säkerhetsplanen ska fastställa funktioner och ansvarsområden för de personer som beviljats tillträde till VIS, inklusive kommunikationsinfrastrukturen.

2. Säkerhetsuppgifter och ansvarsområden för kommissionens anställda, uppdragstagare och andra medarbetare som är involverade i den operativa förvaltningen ska fastställas, dokumenteras och meddelas de berörda personerna. Dessa uppgifter och ansvarsområden ska för kommissionsanställdas del fastställas i arbetsbeskrivningen och målen. Motsvarande uppgifter för uppdragstagare ska fastställas i kontrakt eller tjänstenivåavtal.

3. Avtal om sekretess och tystnadsplikt ska ingås med alla berörda som inte omfattas av särskilda regler för offentliganställda på EU- eller medlemsstatsnivå. Personal som arbetar med VIS-uppgifter ska ha nödvändigt säkerhetsgodkännande eller certifiering i enlighet med de närmare bestämmelser som ska fastställas i säkerhetsplanen.

Artikel 21

Information till personal

1. Alla anställda och, i förekommande fall, uppdragstagare ska i den omfattning som krävs för deras tjänsteutövning erhålla lämplig fortbildning när det gäller säkerhetsmedvetande, rättsliga krav, politik och förfaranden.

2. Det ansvar som åligger anställda och uppdragstagare i samband med att en anställning upphör eller ett uppdrag avslutas ska fastställas i säkerhetsplanen, som också ska omfatta förfaranden för att förvalta återlämnande av egendom och återkalla tillträdesrätt i ovannämnda situationer.

KAPITEL V

SLUTBESTÄMMELSER

Artikel 22

Tillämpning

1. Detta beslut ska tillämpas från och med den dag som kommissionen fastställer i enlighet med artikel 48.1 i förordning (EG) nr 767/2008.

2. Detta beslut ska upphöra att gälla när förvaltningsmyndigheten övertar ansvaret.

Utfärdat i Bryssel den 4 maj 2010.

På kommissionens vägnar

José Manuel BARROSO

Ordförande